CLAIMS

1. A software program to be utilized in an audio or video device by the original equipment manufacturer of the device, the device for playback of encrypted audio or video content residing on a memory card, the software program configured to:

receive commands including a playback command from a user interface of the device;

decrypt encrypted audio or video content from the memory card such that the original equipment manufacturer need only send the playback command from the user interface of the device to the software program and the decrypted audio or video will be played back.

2. The software program of claim 1 wherein the software program is further configured to:

copy location information of the encrypted content into a memory of the audio video device;

access the location information from the memory of the audio video device;

locate the encrypted content within the memory card with the accessed location information.

3. The software program of claim 1 wherein decrypting the audio or video content comprises:

copying one or more encrypted keys from a protected area of the memory card into a memory buffer of the device;

copying encrypted audio or video content from the memory card into a memory buffer of the device;

decrypting one or more of the copied encrypted keys;

decrypting the copied encrypted audio or video content with the one or more decrypted keys.

4. The software program of claim 3 further comprising immediately deleting the one or more decrypted keys after decrypting the audio or video content.

5. The software program of claim 4 wherein about less than one to ten seconds of content is decrypted at a time with the one or more decrypted keys before the one or more decrypted keys are deleted.

6. The software program of claim 4, wherein about two seconds of content is decrypted at a time with the one or more decrypted keys before the one or more keys are deleted.

7. The software program of claim 1 wherein decrypting the audio or video content comprises:

(a) calculating a media unique key; and thereafter

(b) decrypting a title key stored in the memory of the device with the media unique key; and thereafter

(c) decrypting a group of frames; and thereafter

(d) deleting the decrypted title key;

(e) deleting the media unique key; and

(f) repeating (a) through (e) until the entire track is completed.

8. A portable device having a microprocessor, random access memory and a software program executed by the microprocessor, the device configured to:

receive a group of commands including a playback command from a user interface of the portable device;

retrieve encrypted data residing in a removable storage media upon receiving the command;

store the encrypted data in a memory of the device;

decrypt the data; and

output decrypted audio or video content such that the device only need send a command from the group of commands from the user interface to the software program in order to output the decrypted audio or video content.

9. The portable device of claim 8, wherein about two seconds of encrypted data is stored in the memory of the device, and subsequently decrypted before being deleted.

10. The portable device of claim 8, wherein the removable storage media is a solid state memory card.

11. The portable device of claim 8, wherein the removable storage media is an optical disc.

12. The portable device of claim 8, wherein the software of the device is further configured to decompress and decode audio content in either the AAC, MP3 or WMA format.

13. The portable device of claim 8, wherein the software of the device is further configured to:

copy playlist information and track information from the removable storage media into a memory of the device, and

locate the encrypted data to be retrieved based on the playlist and track information within the memory of the device.

14. The portable device of claim 13 wherein the track information comprises for each track:

the number of audio objects comprised by the track;

the first audio object comprised by the track;

the last audio object comprised by the track;

the current audio object being decrypted; and

the offset of the current audio object.

15. The portable device of claim 14 wherein the track information further comprises:

the size of the track in bytes;

the total playback time of the track;

the elapsed time of the track

the current element number within the audio object;

current element of the track to be played;

the offset of the current element;

the total number of elements in the audio object.

16. A method of playing encrypted audio or video content stored in a secure media with a device, the method comprising:

a pre-play process comprising:

copying one or more groups of information regarding the tracks to be played back in to a memory of the device;

a play process comprising:

receiving one more commands from a user interface to initiate playback;

accessing the one or more groups of information from the memory of device;

copying encrypted content from the secure media into a memory of the device according to a sequence based upon information of the one or more groups of information copied into the ram memory;

decrypting the encrypted information from the secure media in a sequence based up on the information of the one or more groups of information.

17. The method of claim 16 wherein approximately less than one to five seconds of the encrypted content is copied and decrypted at a time.

18. The method of claim 16 wherein the one or more groups of information comprise playlist and track information.

19. The method of claim 16 wherein the one or more groups of information specify which playlist is to be played, which track within the playlist is to be played.

20. The method of claim 19 wherein the one or more groups of information further comprises which audio object within the track is to be played, and where the audio object is located within the secure media.

21. The method of claim 20 wherein the one or more groups of information further comprises which element within the audio object is to be played, and which frame within the element is to be played.

22. The method of claim 16 wherein the pre-play process further comprises authorizing the secure media.

23. A system enabling a portable device to access encrypted music on a memory storage device comprising:

one or more application programming interfaces configured to:

receive a plurality of commands from a user interface of the portable device; and

send commands to an isolated security engine, the isolated security engine configured to:

receive commands from the application programming interface;

copy encrypted keys and encrypted content from the memory storage device to a memory of the portable device;

decrypt the keys;

decrypt the content using the decrypted keys; and thereafter

delete the decrypted keys.

24. A method for allowing a device having a processor and random access memory to easily access encrypted data from a memory card with a group of commands, the method comprising:

retrieving playlist information from the memory card and storing the information in the random access memory of the device;

retrieving track information from the memory card and storing the track information into the random access memory of the device;

receiving a command selected from the group of commands from the device, the command accessing both of the playlist information, and track information from the random access memory;

executing the command by retrieving the encrypted data stored within the memory card and decrypting the data based on the accessed information.

25. The method of claim 24 wherein the playlist information comprises:

the name of a playlist;

the playlist name string length;

the playback time of the playlist;

the tracks comprised by the playlist; and

the index corresponding to the playlist.

26. The method of claim 24 wherein the track information comprises:

a track number;

an index corresponding to the track number;

a number of track units in the track; and

the playback time of the track.

27. The method of claim 24 wherein the track information comprises:

a format type of a track;

a sampling frequency of the track;

the size of the track in bytes; and

the current track being decrypted.

28. The method of claim 27 wherein the general track information further comprises:

the number of audio objects comprised by the track;

the first audio object comprised by the track;

the last audio object comprised by the track;

the current audio object being decrypted; and

the offset of the current audio object.

29. The method of claim 27 wherein decrypting the data comprises:

copying one or more encrypted keys from a protected area of the memory card into a memory buffer of the device;

copying encrypted audio or video content from the memory card into a memory buffer of the device;

decrypting one or more of the copied encrypted keys;

decrypting the copied encrypted audio or video content with the one or more decrypted keys.

30. The method of claim 27 wherein decrypting the data comprises:

(a) calculating a media unique key; and thereafter

(b) decrypting a title key stored in the memory of the device with the media unique key; and thereafter

(c) decrypting a group of frames; and thereafter

(d) deleting the decrypted title key;

(e) deleting the media unique key; and

(f) repeating (a) through (e) until the entire track is completed.

31. A software system that enables a device to access content on a secure medium comprising:

one or more user interface modules for receiving commands from the device;

an applications programming interface for receiving the commands from the user interface module(s) and managing the retrieval and storage of both encrypted and non encrypted content from the secure medium;

a security engine for decrypting the encrypted content and encrypted keys sent from the secure medium to memory of the device, the decrypted keys used to decrypt the encrypted content, and wherein

one or more of the keys are contained in a first encrypted data segment, and

encrypted content is contained in a second encrypted data segment, and

the security engine buffers and decrypts a portion of the first data segment, buffers and decrypts the second data segment, and thereafter deletes the decrypted one or more keys before decrypting the, such that decrypted keys are in a decrypted state for the time it takes to decrypt less than one to about five seconds of content.

32. The software system of claim 31, wherein the key is in a decrypted state for the time it takes to decrypt and process about two seconds of content.

33. The software system of claim 32, wherein the content is encoded in the form of AAC, MP3 or WMA.

34. The software system of claim 31, wherein the portion of the first data segment buffered and decrypted is about 512 bytes.